## REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

In response to the objection to claims 11-15, these claims have been cancelled so as to obviate this ground of objection.

In response to the rejection of claims 1-15 under 35 U.S.C. §112, paragraph 1, all independent claims have now been amended so as to avoid recitation of a "pathname". Instead, the claims now refer to the request as including a "file name".

Although the original specification describes the request in terms of a uniform resource locator (URL) which points to a given Web page, those skilled in the relevant art as of applicant's priority date (March 31, 1999) clearly understood a URL to include a file name. Of course, a domain name part of the URL will also be present and must be resolved to identify the computer to which a request is directed. As those in the art also well appreciated at that time, a file name may take the form of a pathname.

A copy of pages 692-693 from a 1996 Edition of "Computer Networks" by Tanenbaum makes such explicitly apparent and it is respectfully submitted that one of ordinary skill in the art reading the applicant's original specification would clearly understand that a file name (or, for that matter a pathname) would be included as part of the request URL that is being described in the original specification text.

Accordingly, the specification has been amended at page 11 so as to make a more explicit explanation of that which would have been inherently understood by those having ordinary skill in the relevant art at the relevant time. It is not believed that such amendment therefore constitutes any "new matter".

The independent claims have also been amended to remove the earlier recited comparison aspects. In applicant's exemplary embodiments it is actually hashes that are being compared -- one of such being a decrypted digitally signed hash.

The rejection of claims 1-10 under 35 U.S.C. §103 as allegedly being made "obvious" based on Farber '791 in view of Brickell '716 is respectfully traversed.

The Examiner continues to argue that a skilled person starting with Farber would see that one could 'beef-up' the security of the system by digitally signing the 'True Name' of a file and using that digital signature in place of the 'True Name'. It is respectfully submitted that such is not the case. Indeed, as will be explained below, Farber teaches an approach so insecure that it is easily susceptible to an attack of the very sort which applicant's invention is designed to prevent.

In Farber, normal' file names (e.g. US Response.doc) are not used. Instead 'True Names' are used - for example '9e107d9d372bb6826bd81d3542a419d6' which just happens to be the result of applying the MD5 hashing algorithm (Farber, col. 13, lines 13 and 14) to the phrase 'the quick brown fox jumps over the lazy dog', expressed in hexadecimal notation.

Names like '9e107d9d372bb6826bd81d3542a419d6' are clearly different from normal file names like 'US Response.doc'. For example, '9e107d9d372bb6826bd81d3542a419d6' is fundamentally dependent on the content of the file (i.e., it is calculated from the file content), whereas there is no such direct relationship between normal file names like 'US Reponse.doc' and all the data contained in the so-named file. Farber actually points out this distinction (col. 2 lines 12 to 16).

The amended version of the independent claims requires that the file name used in a request has no such direct calculable relationship to the contents of the file.

An advantage for human users of filenames (path names) like web/offices/com/speeches/08-18.htm over using filenames like '9e107d9d372bb6826bd81d3542a419d6' are clear. Indeed, the latter would be unusable unless human users were presented with an indication of what the file named '9e107d9d372bb6826bd81d3542a419d6' was. Col. 35 lines 38 to 61 of Farber appear to suggest some sort of directory which converts a user request for file web/offices/com/speeches/08-18.htm to a machine request for file '9e107d9d372bb6826bd81d3542a419d6'.

However Farber's security is weak in that anyone can take a file and calculate its MD5 hash. Indeed, Farber itself says that this must be easy to do - see col. 13 line 5. So, in the attack scenario contemplated by the applicant here, where a malicious user has gained user rights on a server computer, the malicious user could rewrite file web/offices/com/speeches/08-18.htm to include an egregious speech, have the file 'assimilated' - which involves calculation of that file's 'True Name' - i.e. the hash of the files contents, and then publish a reference web/offices/com/speeches/08-18.htm which points to the altered file (col. 35 lines 38 to 61).

What the applicants have appreciated, and what Farber did not, was that by having users digitally sign the files they create, this kind of malicious user can be foiled since they could never apply an acceptable digital signature to the file.

Even in the unlikely event that a skilled person did introduce digital signatures into Farber, they would follow the example of the prior-art and introduce the digital signature check at the computer receiving the file, not at the computer serving the file (as applicant's claims require).

Unsurprisingly, that is exactly what Brickell '716 proposes - see column 1 lines 45 to 50. More generally, since col. 1 of Brickell draws an analogy with handwritten signatures on commercial documents, the skilled person reading Brickell would only think of checking the digital signature at the recipient. In what commercial situation does the sender of a commercial document check that the signature is authentic? None that come to mind.

The only references to Farber newly cited by the Examiner are col. 38 lines 1 to 4 and col. 5 lines 37 to 41 (see last line of page 4).

Col. 5 lines 37 to 41 discusses the prior-art, not what is proposed by Farber (a comparison with col. 2 lines 12 to 16 should make that clear). Col. 38 lines 1 to 4 say nothing about a network. All the sentence referred to by the Examiner means is that the pathname is 'followed'. For example a computer presented with the pathname web/offices/com/speeches/08-18.htm would first go to the directory called 'web', then to the directory 'offices' within the web directory, then etc. etc. All of that takes place on a single computer - which uses 'normal' pathnames internally (see col. 6 lines 11 to 16) but hides those from remote computers. To see this, note that none of the 'Remote Mechanisms' described at col. 23 line 26 to col. 26 line 7 of Farber use 'normal' file names or pathnames.

Given such fundamental distinction in all independent claims from either of the cited references (whether taken singly or in combination), it is not believed necessary at this time to discuss further deficiencies of these references with respect to other features of the rejected claims.

Accordingly, this entire application is now believed to be in allowable condition and a formal Notice to that effect is respectfully solicited.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By: Larry S. Nixon
Larry S. Nixon
Reg. No. 25,640

LSN:vc
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100